View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Repository of the University of Namur

Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche

researchportal.unamur.be

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Data Protection - Belgium

Dhont, Jan; Poullet, Yves

Published in:
Computer Law and Security Report

Publication date:
2000

Link to publication

Citation for pulished version (HARVARD):
Dhont, J & Poullet, Y 2000, 'Data Protection - Belgium: an analysis of the new law', *Computer Law and Security Report*, vol. 16, no. 1, pp. 5-19.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 13. Nov. 2019

DATA PROTECTION — BELGIUM

AN ANALYSIS OF THE NEW LAW

THE ACT OF 11 DECEMBER 1998 TRANSPOSING THE DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND THE FREE MOVEMENT OF SUCH DATA: A CONCISE EVALUATION.*

Jan Dhont and Yves Poullet

Privacy protection is a fairly new issue in the Belgian legal system and is in the course of continuous development. The growth to maturity seems, however, far from being attained yet, due to economic and political constraints, though also because of a lack of adequate conceptualisation of the notion of 'privacy'. This article examines the implementation of the EC data protection directive in Belgium and the problems that still remain in its integration into Belgian law.

1. INTRODUCTION

Privacy is firstly and in general protected by Article 22 of the Belgian Constitution stating that everyone has the right of respect of his private and family life, unless in the cases and under the conditions determined by Act of Parliament.[1] A curtailment of the privacy of the citizen needs a democratic foundation and should be debated in Parliament. Further, it is generally accepted that Article 8 of the European Human Rights Convention has a direct effect.[2] This article of the Convention and the case law of the Court of Strasbourg form a very important guideline for solving conflicts and for the interpretation of rules. Furthermore, privacy comes up in different contexts, and case law in different domains, of social interaction, e.g. the rules of professional secrecy,[3] the right of depiction, the legislation guaranteeing the transparency of public documents,[4] the prohibition of installing an opening in a common wall,[5] the Act(s) protecting the secret of communication,[6] etc.

The explosive evolution of information technology has, however, given birth to more specific legislation regulating the protection of personal data. Belgium signed on 7 May 1982 the Convention nr. 108 of 28 January 1981 concerning the protection of persons for the automatic processing of personal data, concluded in the Council of Europe. The Convention was ratified by the legislative act of 17 June 1991.[7]

In 1976, the then responsible Minister of Justice, Herman Vanderpoorten, introduced a Bill.[8] It lasted, however, until 8 December 1992 before the first data protection Act was enacted. The reason for this delay was probably the introduction of the Act of 8 August 1983 organizing a State Register.[9] This Act contained some dispositions concerning respect for private life, more precisely according to the right of access and rectification, and also installed a monitoring arrangement.

With the creation of the Crossroad Bank for the Social Security, the problem of data protection again became of topical interest. The Act of the 15 January 1990 constituting this public organ contains some provisions concerning data protection and installed the Privacy Commission. This authority achieved — after the broadening of its field of competence in many other Acts[10] — its final form in the data protection Act of 8 December 1992 (hereafter: the previous data protection Act).[11]

This Act laid down — *in general* — the same principles as can be found in the Directive 95/46/EC,[12] though used at some points other wording and concepts (cf. *infra* nr. 4 and ff.). The most important difference is that under the previous data protection Act the processing of personal data was always allowed, unless prohibited by the law; reasoning which is inverse to that which is the basis of the Directive. Many Royal decrees were issued determining and specifying the concrete methods by which the law had to be respected. Some of these adhered to an interpretation that anticipated the implementation of the Directive.[13]

Nevertheless, the previous data protection Act showed many deficiencies and the obligations seemed sometimes difficult to respect in reality. Unfortunately no systematic evaluation of this act was made, notwithstanding the fact that the period between 8 December 1992 and 11 December 1998 is conceived as a period of trial.[14] This may lead to the same obstacles as under the previous Act and will surely not enhance the quality of the most recent law.

The new data protection Act forms the first part of the implementation of the European legislation. As will be seen further the Directive 97/66/EC — forming the second part — is far from being transposed yet.

Furthermore, it is both striking and surprising that practically no parliamentary debate was held, for a matter involving the liberties of the citizens.[15]

The original text of the Bill has been amended at some important points in the text following the advice of the

ISSN 0267 3649/00/$20.00 © 2000 Elsevier Science Ltd. All rights reserved

privacy Commission and the Council of State, though was never evoked by the Senate.

A Royal decree is in course of preparation and will integrally execute the new data protection Act.

2. THE DATA PROTECTION ACT

2.1 Definitions of the Act

The personal and material field of application of the Act of 8 December 1992 is determined by the content of the main concepts underlying this regulation. Because many and important changes are introduced, some of these key concepts will be treated first in order to render a good understanding of the scope of the new data protection Act possible.

At the level of the definitions, it may be said that — apart from eventual minimal semantic deviations due to translation — the text of the Directive is mostly copied by the Belgian legislature.[16]

In comparison with the former version of the data protection Act, *personal data* is defined much more precisely. Where personal data was defined as *data*[17] relating to an identified or identifiable physical person,[18] the new text states what should be understood by 'identifiable': viz. "*is considered identifiable a person who can directly or indirectly be identified, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.*"[19]

Although this precision seems at first sight not to be changing the nature of 'personal data' very much (i.e. data that is related to an identifiable natural person), one should be careful not to have 'myopic' vision on this matter. Before the passage of the Directive, one had to ask oneself if the controller could, with reasonable means, identify the persons to which the data was related. If he received data from an intermediary that rendered the data anonymous, he could not, without reasonable means, deduce to whom it was related, and that the data protection legislation was not applicable to him.[20] The Explanatory Report adheres, however, to another vision. Referring to Recital 26 of the Directive,[21] one should check if reidentification is *in abstracto* reasonably possible.[22] If the controller gets information which is 'rendered anonymous', though he himself, the supplier, or any other third entity can with reasonable means identify, the data should be qualified as 'personal data' on account of the above mentioned controller. The result of this is first that what was before called anonymous, will not necessarily be so any longer under the new Act which will elicit the application of the latter; only when the process of anonymity is absolute and irreversible will the Act not be applicable.[23]

The notion of *processing* is fundamentally reformulated. The wording of the former data protection Act was not correct by reserving the notion *processing* merely for the *automatic processing* of personal data, apart from the *holding of a manual filing system*.[24] Henceforth, processing means "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*"[25]

Thus the definition, and by consequence, the field of application of the Act of 11 December 1998 is much broader.

Firstly, the pure collection of personal data falls under the data protection regime established by the new Act.[26] Further, it seems that the enumeration of different operations that are mentioned in the definition is open ended, which can be welcomed bearing in mind the continuous evolution of the technologies.[27]

Secondly, even if only one operation is done with personal data, this should be qualified as a processing.[28] It is thereby not longer important to ask oneself if the processing is or is not done by automatic means. The pure manual collection of personal data will be legally defined as *processing*.

Although this enlargement of the content of *processing* will in some cases be necessary for an adequate privacy protection, the consequent application of the legislation will in other hypotheses be problematic. We think of the simple consultation of a databank online or of a Web page on the Internet. This will lead to the exercise of consultant obligations,[29] in many situations where not only the privacy of another data subject is endangered but also the privacy of the 'surfer'. One could ask what the meaning is of the obligation to inform or the obligation to notify the Privacy Commission if the consulted data were not conserved or recorded by the consultant?[30]

Under the previous Act the notions of *processing* and *purposes* were synonymous.[31] This is logical, if personal data is stored and processed in different physical places, the principle of finality will apply to the whole processing apart form its physical or logical structure. Processing and purpose are therefore closely linked up. The Act of 11 December 1998 seems, however, to indicate that one processing could serve a multitude of purposes.[32] Here again, one cannot dissociate both notions. If one allows that personal data can be processed for different purposes, this could only happen legitimately so long as the purposes are not mutually incompatible. This leads firstly to the already before recognized theory that a processing can be connected with a *generic* purpose. A processing can serve several purposes that are somehow interconnected or *closely related* though this will be requalified as a unique but generic purpose. Without that the application of the finality principle would become obsolete and impossible. Secondly, the fact that one operation can constitute a processing renders everything free of complication. The Explanatory Report creates a lot of misunderstanding in considering a sole operation unconditionally as a processing.[33] It can only be concluded here that the text of the European and Belgian legislature is very ambiguous concerning this point, and will for pragmatic reasons not change the idea that one processing corresponds to one (be it generic) purpose.

The notion of *filing system* has also been altered.[34] In comparison with the former Act of 8 December 1992, the definition of a filing system is slightly more precise; the personal data should be accessible according to specific criteria. What criteria should be taken into account is, however, not determined, which enhances legal uncertainty.[35] Recital 27 of the Directive states, however, that *the content of a filing system must be structured according to specific criteria relating to*

individuals allowing easy access to the personal data. The category of 'specific criteria relating to individuals' can, however, still be quite broad and does not merely refer to identifying data. It is a pity that the Belgian legislature did not follow the advice of the Privacy Authority to elaborate a clearer definition and to give explicit examples so as to avoid further controversy about this point.[36,37]

The *controller* and *processor* replaced the former 'holder of a filing system' and the 'controller of the processing' (Fr.: 'gestionnaire du traitement').

With regard to the definition of the *controller* three important specifications and/or changes are introduced[38]:

A public authority is explicitly mentioned as an entity that can function as controller. No specific reference is, however, made to an agency.[39]

Where under the former version of the data protection Act, the controller was the entity that was competent to decide about the purpose *or* about the sorts of data that constitute a processing, the new Act speaks about the natural or legal person, de factual association or public authority that is competent for the purpose *and* the means of the processing of personal data. Both criteria (purpose[40] and means) are cumulative which could cause many problems as it may happen that in reality different entities decide on the purpose and the means of a processing.[41]

The decision concerning the purpose(s) and means of the processing can be taken by parties *alone or jointly with others*. So it is possible that if two or more parties decide upon the purposes and means of a processing, they will all be carrying the full responsibility of a controller.[42] Each of them could be sued separately when neglecting the provisions of the Act. It is, however, also possible that the same entities stand out as one legal body in which case the latter will be the controller.

The *processor* could be every natural or legal person, factual association or public authority that processes personal data on behalf of the controller.[43] This could be a contractor who makes some profiles for a direct marketing office, a private enterprize that manages the data for another enterprize or public authority, etc. Persons that fall under direct authority of the controller fall outside the definition of processor.[44] This means more concretely that if there exists an employer-employee relationship between the controller and the person that factually processes the data, the latter will not be qualified as a processor.

Finally, the concepts of *third party*, *recipient* and *the data subject's consent* are in conformity with the Directive introduced.

The *third party* is every physical or legal person, public authority or factual association other than the data subject, the controller, the processor and those persons that are placed under direct authority of the controller to process the personal data.[45] The notion of third party is not totally new and figures already in the Royal decree nr. 13 of 12 March 1996 that determine the conditions under which an exception could be made to the obligation of notification.[46]

The *recipient* is the entity to whom the personal data are disclosed, whether it is a third party or not.[47] This notion makes it possible to 'fine-tune' some rules in order to obtain a better transparency in the processing of personal data. For instance, it may happen that data is transferred from one department to another, of the organization that is qualified as controller. It will be likewise under the different departments in a hospital. In these circumstances it might be necessary for that data subject to be informed about the transferral in order to guarantee fair processing.[48,49] In the context of the notification the new Act requires also that the identity of the recipients to which the information could be potentially disclosed should be declared in the notification form.[50]

Authorities that are susceptible to receiving data in the context of a particular inquiry will not be qualified as a recipient. This exception has to be interpreted restrictively and applies merely to special inquiries that were not foreseeable.[51]

Finally, the Act describes what should be understood by 'the data subject's consent': *"every manifestation of the free, specific and informed will by which the data subject or his representative accepts that the personal are the object of a processing."*[52] A good and clear understanding of this notion will be mandatory because many key provisions make reference to it. Article 8 states for instance that the processing of personal data is only allowed if the data subject has unambiguously given his consent; furthermore, the principled prohibition to processing sensitive personal data can in some circumstances be circumvented if the data subject gives his — written — consent.[53]

The consent should be given freely, i.e. without any direct or indirect constraint on the data subject. This will, however, mostly be an ideal that does not correspond to the reality where power relations or economic factors interfere with free consent. The specific character of the consent is also intended to protect the data subject since a consent that is too vague or that makes allusions to purposes that are circumscribed too broadly, will not be considered as consent at all.

The consent must have an informatory character. This implies that all necessary information should be given to the data subject in order to render the first two aspects of the consent possible and, moreover, to guarantee that in the context of a particular case the rights and freedoms of the data subject are respected.

2.2 Field of application of the new act

Ratione materiae and personae

Article 3, §1 of the new data protection Act provides that the Act is applicable to the processing of personal data wholly or partly effected by automatic means, and to every non-automated processing of personal data that is included or intended to be included in a personal data filing system.

With analogy to the former Act it can be assumed that mixed processings, i.e. processings that are related to a combination of non-personal and personal data will fall under the scope of the Act. Furthermore, legal persons are excluded from every protection of the Act; only physical persons are granted protection.[54]

Paragraphs 2-5 of Article 3 of the new Act lists some total or partial exceptions to the field of application. They will be examined briefly below:

Paragraph 2 reiterates the position from the previous Act that the processing of personal data by a natural person in

the course of *purely personal or household activities* falls outside the scope of the Act. Two old provisions are omitted positing that the Act does not apply to processing of personal data falling under a prescript of publicity and (secondly) stating that the Act is not applicable purely to processing of personal data made public by the data subject — as far as the processing relates to the purpose of the disclosure. This may be welcomed because the two provisions could hardly be strictly applied.[55]

The third paragraph of Article 3 contains four categories of exceptions concerning the *processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression* and intends to transpose Article 9 of the Directive. A regulation of this matter would be welcomed because the previous Act did not provide for any exceptions in favour of processing for journalistic means that lead to a *de facto* non-application of the Act.[56]

The general rule remains that processing for the purpose of journalistic, artistic and literary expression fall within the domain of the Act. However, some very specific and well-determined exceptions are developed. No distinction is made between journalistic purposes on the one hand and artistic and literary expression purposes on the other.[57]

The ultimate condition in which Article 3, §3 finds application is that the processing serves *"solely purposes of journalism, or artistic or literary expression"*. Although the Council of State offers more clarity in the text about these finalities, the Act gives no guidance as to precisely what should be understood by *"purposes of journalism* and *artistic or literary expressio"*.[58] The most reasonable interpretation will, however, be to follow a functional approach. The data protection legislation does not regulate some categories of professions though is directed to the regulation of (the purposes of) processing. It is about the exemption of certain processing of which the finality is the production of an expression for communication to the public of which the aesthetic, intellectual or informational quality is affirmed. If this interpretation is followed, one does not necessarily need the quality of a journalist, writer, etc. to fall under the exemptions.

(a) The first exception nullifies Articles 6, 7 and 8 of the Act which establish a protection regime for sensitive data if the processing is related to personal data that is obviously made public by the data subject or is closely related to the public character of the data subject or with the fact into which this person is involved.[59] These criteria that are derived from the Jurisprudence of the European Court of Human Rights lead to a case-by-case evaluation or judgement *in concreto.*

(b) The second exception determines firstly that Article 9, §1 is not applicable to the processing of the data if this would prevent the collection of data near the data subject.[60] Article 9, §1 fixes the duty to inform the data subject in case of a primary data collection. The *ratione legis* of this rule is to allow *undercover* journalism in these circumstances where it is reasonably permissible and of relevant societal interest.[61] Secondly it is stated that Article 9, §2 — which contains the conditions relevant to the duty to inform in the case of a secondary data collection — will not apply if the application of this article would lead to the following results:

- the collection of data would be prevented;
- the intended publication would not take place;
- the application would provide indications about the sources of the information.[62]

(c) The third exception concerns the Articles 10 and 12 of the Act, regulating the right of access and rectification of data.[63] Here also these articles will be neutralized if their application would prevent the intended publication or would provide indications as to the sources of the information.

(d) The fourth exception is unconditional.[64] Where the controller of a processing serving a 'journalistic' or 'artistic' goal is required to notify (cf. *infra* nr. 29), he should not inform the Privacy Commission about the prior background to the information and the exercise of the right of rectification towards the data subject, any more than the motives on which he relies to facilitate the commented disposition. This processing will not be maintained in the register of automatic processing conserved by the Privacy Commission. Finally, the stipulations concerning the transfer of personal data to third countries will not find any application with regard to processing for journalistic, artistic and literary purposes.

The fourth paragraph provides some exceptions in favour of processing for public security purposes.[65] Where the Directive connects the exemption to *purposes* of public security, defence, State security, etc., Article 3, §4 refers to *processing of personal data of the State Security, the General Service of Information and security of the Army, the security Authority, the security officers and the Fixed Comity on the information services and the Service Inquiries thereof.* Although the last sentence states that one can only rely on the exemptions *as far as they are necessary for the exercise of their mission*, the connection of the exceptions with a certain security service instead of a security purpose, implies a deviation from the functional approach of the Directive and therefore does not seem correct. The exceptions can only be invoked as far as a processing of one of the mentioned services serves a public security purpose.

The list of exceptions is quite long and include nearly all the dispositions of the Act. The following are thus *not* applicable: in principle, the rules concerning the prohibition of sensitive personal data laid down in the Articles 6-8 of the new Act; the obligation to inform the data subject (Article 9); Articles 10 and 12 concerning the right of access, rectification and opposition; Article 14 related to the action of suspension; the obligation to notify at the address of the Privacy Commission and the possibility of a prosecution by this authority on account of a complaint thereto as provided in Article 31, §§1 to 3. Moreover, Article 17*bis* of the new Act is not applicable here, which means that no special additional protective measures can be implemented by Royal decree for processing for public security purposes.

Although the fact that the rules concerning the quality of the data and the lawfulness of the processing remain applicable with regard to this category of processing, the level of protection will in reality be quasi non-existent.[66] Strangely enough no discussion took place in Parliament *vis-à-vis* this paragraph; nor did the Council of State or the Privacy Commission present views on this matter implying that the fundamental liberties of the citizens were not respected.[67]

The fifth paragraph of Article 3 contains some general exemptions from the duty to inform and the right of access and rectification according to processing kept by public authorities (mostly *police services*) in the light of their

mission as judicial and administrative police. An "indirect" right of access and rectification is granted to the data subject, bypassing the Privacy Commission. Here too, this right will be obsolete because the citizen will mostly not know if and where his personal information is processed.

The last exception concerns the *European Centre for disappeared and sexually exploited children*[68] and formed the source of long debates in the Chamber.

The Centre is after authorization by Royal decree (deliberated in the Council of Ministers) delivered from the rules concerning the processing of sensitive data — with the exception of Article 7 (health data) — and the duty to inform, the right of access and opposition.[69] The exception is only valid for the reception, the transmission to the judicial authority and the succession of the data concerning a crime or outrage involving suspected persons in a case concerning disappearance or sexual exploitation. A Royal decree ordered after consultation with the Privacy Commission, will determine the duration and condition of the authorization.

Ratione loci

Article 3*bis* 1° of the new Act introduces a new criterion of connection in order to fix the field of application *ratione loci*. The criteria of the previous data protection Act needed to be revised in a context of growing internationalization of social communication in all its facets.

The distinction between an automated as opposed to manual processing is no longer relevant in order to decide if the Belgian Act should be applied. Nor is the locality of the processing.[70] The central criterion is the place of the fixed establishment of the controller; the Act is applicable if the processing is "*effected in the frame of the real and effective activities of a fixed establishment of the controller on Belgian territory or on a place where Belgian law is applicable on account of the international public law.*" [71] Two conditions must be complied with before the Belgian law will be applicable:

(i) Firstly, the processing should be effected in the frame of the real and effective activities of a fixed establishment of the controller. So, it will be the law of the territory where the establishment is situated *and* for which the processing is effected that falls under the application of the Act.[72] For the sake of clarity, one will have to check in which controller's establishment the processing is done, and on what territory this establishment is based. It may frequently occur that the processing will *de facto* take place in Belgium, on behalf of a foreign establishment in which case the law of that (EU) country will apply. Furthermore, if a foreign enterprise processes personal data on foreign territory, it will not be submitted to the Belgian law if the processing is not realized in *the context of the activities* of the subsidiary company, even if that subsidiary is based in Belgium.[73]

(ii) Secondly, it is required that the establishment of the controller for which the processing is done must be situated on Belgian territory. The Explanatory Report refers explicitly to Recital 19 of the Directive, which states that: "*whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements.*" This Recital continues: "*whereas the legal form of such an establishment whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect.*"

Article 3 *bis* 2° of the new Act provides for a second criterion of connection should the first not find any application. The situation that is anticipated is one where the controller has no establishment on the European territory but "*uses equipment for the processing of personal data automated or otherwise, that can be localized on Belgian territory, other than those used only for the transit of personal data over Belgian territory.*"[74]

Although this rule is well intended in order to make the protection as broad as possible, it could lead to difficulties when a literal interpretation is followed. From the very moment that the controller has no establishment on the community territory, but uses any possible means[75] localized on Belgian territory to process personal data, Belgian law will apply (except when the means are used for the pure transfer of personal data). If a physical link could be made between a processing that is situated outside the European Community and Belgium, Belgian law will apply, however minimal this link may be. For example, the processing of personal data realized by a Web site of which the server is situated in another part of the world would fall under the scope of the Belgian law if the site would allow the collection of data by means situated on Belgian territory (e.g. the PC of the surfer). This view seems unrealistic and undermines the effect of the new Act.

Therefore a second interpretation can be justified that respects the *ratio legis* and the other rules of the Act, mainly these relative to the transmission to third countries of personal data. Two hypotheses could be retained where Article 3 *bis*, 2° would be applicable.[76]

The first one alludes to the situation where the controller seeks willingly to escape the national law taken in the light of the Directive, and therefore, relocates his establishment in a third country while still using certain facilities within the community territory. The second points to the case where the controller diverts data towards a third country for further processing, by means of an intermediary situated within the European territory.

The goal of Article 3 *bis*, 2° is to protect the data subject against any lack of protection emanating from the relocation of the establishment of the controller.[77] This ratio corresponds to the text of Recital 10 of the initial proposal for a Directive, which lies at the foot of the current Recital 20.[78]

The rules on the transborder flow of data to third countries will be applicable in most of the other hypotheses where personal data are processed by a controller who is not established in the community. If the transmission starts from Belgian territory, Articles 21 and 22 of the new Act apply to every person involved. (cf. *infra* nr. 31). Consequently, the data subject is not left without protection. If, however, the controller intervenes only when a third country without intermediary becomes involved because technical means situated on Belgian territory render such transfer possible, Article 3 *bis*, 2° will apply.

Ratione temporis

Article 52 states that the provisions of the new Act will take effect on the date provided by Royal decree. Furthermore, the

King determines the period within which the controller should comply with the terms of the law for these processings that are already existing at the moment that the law comes into operation.

Article 58 of the draft version of the Royal decree fixes the date of operation at the fourth month after its publication. The second paragraph of the same article states that controllers of new and already existing processings should from the same day respect the provisions of the new Act.

2.3 General principles governing the data protection regime

The general principle that personal data may be processed only for "specified, explicit and legitimate purposes" and insofar as these data are "adequate, relevant and not excessive in relation to the purposes for which they were collected and/or further processed" was already incorporated within the previous data protection Act.

In compliance with the requirements of the Directive, the Act of 11 December 1998 has elaborated these two principles more extensively.

Under Article 4 of the new Belgian Act, different and more precise principles are worked out. These include: the principle of "fair and lawful processing"[79]; the "purpose specification principle" and the "use limitation principle"[80]; the "compliance principle"; the "data quality principle" and finally the "conservation principle".

Article 5 of the same Act develops the criteria for making data processing legitimate. The content of this article is in strict conformity with the European provision (Article 7). It must be stressed that a Royal decree can specify certain cases where the balance between the legitimate interests of the controller in carrying out the processing and the data subject's interests or fundamental rights might be disrupted, in which case the processing will be expressly forbidden.

Special categories of data

The previous version of the Belgian Act did envisage three separate categories of sensitive data. The first category included "data concerning racial or ethnic origin and religious or philosophical beliefs and data concerning sex life"[81]. The second concerns data relating to health, which means any information about the physical and mental state of an individual.[82] Finally, there is the criminal records category[83].

The distinction is maintained under the new Belgian Act, but contrary to the approach proposed by the Directive that puts together the three categories in a same article.

The data listed in the new Article 6 as a "special category of data" are explicitly defined by the Directive and encompass all data "revealing" (the previous wording was "concerning" and not "revealing") racial or ethnic origin, religious or philosophical beliefs and data "concerning" sex life. According to statements of the Minister of Justice, any data (e.g. pictures, the simple family name) from which the racial or ethnic origin of a data subject may be deduced will, from now on, be considered as sensitive data.[84]

On the contrary, Article 7 dealing with *health data* does adopt a restrictive definition of the notion. Only data directly concerning the physical or mental state of an individual whether past, present or future are considered to be falling under this provision.[85]

With regard to these two first categories of sensitive data the principle and its exceptions are the same. Derogations to the prohibitions on the processing of such data are explicitly provided by the Belgian Act. We will comment only on those peculiarities of Belgian regulation that extends beyond European provision. According to the first exception, the European concept of "explicit consent" has been replaced by "written consent". A broad exception for the "Social Security System" has been expressly added. The derogation for medical purposes in the absence of the data subject's comment does refer to the European condition that sensitive data are processed by "health care professionals".[86] This notion, however, is not defined[87] and the European requirement that these persons are covered by professional secrecy or an equivalent obligation is strangely met by the fact that the new Belgian Act creates novel penal sanctions for this category of persons.[88]

With regard to criminal records, the Belgian Act considerably extends the scope of the specific protection proposed by the Directive. Whereas the Directive merely establishes special rules for the processing of data relating to offences, criminal convictions or security measures, the Belgian Act adds criminal records including suspected persons to the category of sensitive data and provides derogations only in very limited cases. So, under the Belgian Act, for example, a credit card company is not entitled to set up a list of people suspected of forgery except where expressly provided by legislation.

Hereafter we analyse briefly the rights of the data subject emanating from the Directive.

2.4 The rights of the data subjects

The right to be informed

Article 9 of the new Act contains the obligation to inform the data subject about the processing of his personal data. This is one of the main pillars of the transparency principle.

The first paragraph focuses on the situation where personal data is *obtained*[89] from the data subject (primary data collection), while the second paragraph considers the case where the data is obtained more remotely (secondary data collection).[90]

In both cases the controller should supply the data subject with some minimal information, more precisely: the name and address of the controller (or his representative if any), the purposes of the processing and, if the intended processing serves a direct marketing purpose, the existence of the right to object (free of charge).[91] Some supplementary categories of information should in principle be communicated; i.e. the recipients or categories of recipients of the data, whether replies to the questions made are obligatory or voluntary, as well as the possible consequences of failure to reply, and the existence of a right of access and rectification concerning the data subject.[92] This information should be given unless this is — taking into account the specific circumstances in which the data is obtained — not necessary to guarantee fair processing in respect of the data subject.

The duty to inform can be broadened by Royal decree and after advice of the Privacy Commission depending upon the specific character of the processing.[93]

The formulation of the new Article 9 is much more flexible than the wording of the previous Act. Information should only be given where the data subject has not yet been informed. One can imagine that in most cases the controller will not know the answer to this in which case he will tend to supply the information bearing in mind that failure to comply is punishable.[94] The Explanatory Report further explains that if it is impossible at a given moment to provide complete information, e.g. because the recipient is not yet known or in a case of emergency, where complementary information may be given later.[95]

The fact that the personal data is obtained via the data subject or not will be a determinant of the *moment* when the information should be communicated. In the case of a primary data collection, the information should be given at the very latest when the data is obtained; whereas in the case of a secondary data collection, this moment is moved to the registration of the data or, when communication to a *third party* is considered, to the point of the first communication. When the processing is done for direct marketing purposes, the data subject should be informed *before* the data is first communicated or used on account of third parties for these purposes. The Privacy Authority has made it quite clear that if information is only given when the data is registered by the third party, the right of opposition would effectively become obsolete.[96]

When one deals with a secondary data collection, two exceptions to the duty to inform are foreseen:

(a) where, more precisely for statistical, historical or scientific research purposes or for population research or for the protection and enhancement of public health,[97] notifying the data subject would seem impossible or involve a disproportionate effort.[98,99]

(b) when the registration or communication of personal data is made in compliance with an exception prescribed by Act or secondary legal norm.[100] The wording of this exception to the obligation to inform is much broader than that mentioned in article 11.2 of the Directive, precisely because no information is needed *if recording or disclosure is expressly laid down by the Act or secondary legal norm.* The new Act, for instance, makes it possible to deviate from the present obligation on grounds of state efficiency by a rule that has not been discussed in Parliament.

The conditions for application of both exceptions have to be taken by the King. One could make a similar criticism that appropriate safeguards have not been the subject of serious debate.

The right of access, rectification and opposition

Article 10 of the new data protection Act contains provisions concerning the right of access of the data subject. He should be informed of the fact that data about him is being processed and at least about the purposes for this processing, the categories of data concerned and the categories of recipients to whom the data may be communicated. Furthermore, the controller should give — in intelligible form — all data that is undergoing processing, as well as all the available information about the source of the data. He should also communicate the logic involved in any automatic processing of data concerning the data subject. Finally, the data subject must be informed as to the possible action he can take and of the fact that he can examine the public register kept by the Privacy Authority.

To obtain access to his personal data, the data subject must make his enquiry by dated and signed letter at the address of the controller or any other person designated by the King.[101]

The information should be given immediately or at least within 45 days following receipt of the demand.

A criticism could be that the Belgian legislature failed to specify — as mentioned in Article 12 of the Directive — that access is available *without constraint.* It is not unrealistic, for instance for a third party (e.g. an insurance company or a potential employer) to put pressure upon a data subject in order to obtain information about his medical or other history.

The second paragraph of Article 10 concerns the right of access to health data. The new Act states that every person has the right to obtain knowledge, by direct means or with the help of a health professional, about personal data relating to his health. The communication can take place through the mediation of a health professional chosen by the data subject on the specific demand of the controller[102] or on request of the data subject.

A special exception to the right of access in the context of the processing of health data for medical-scientific means is provided for in the third section of the second paragraph of Article 10 in order to facilitate *double blind testing.*[103] The communication can be delayed if there is no apparent danger of any encroachment upon the privacy of the data subject and if the data are not used to take measures or draw conclusions with regard to the *individual* data subject.[104] The same applies if the data is processed for such medical-scientific purposes, though only so far as access would seriously complicate or hamper the research activity. The data subject should, however, be granted access when the research project is complete.

In that case the prior and written consent of the data subject should be obtained so that his data can be processed for medical-scientific purposes and so that access rights will not be exercised during the research activities.[105]

No response should be given to a data access request on behalf of the data subject, until after the lapse of a reasonable period. The question, however, is what a "reasonable interval" might be? Much will depend on the context of the processing of personal data. For example, it could be envisaged that the lapse will be shorter in a medical context where the trust relationship between health professional and patient is prevalent.

Article 13 makes provision for *indirect access* and rectification for processing arising rom public security and police activity as mentioned in Article 3, §§ 4 to 6.[106] Every citizen can ask the Privacy Authority to check and verify whether his personal data has been correctly processed by the controller. No detailed information is given to the data subject. The latter will simply be informed that the "necessary verifications are done".[107] However, in the case of processing of personal data involving an identity control, more specific information can be given, provision for which must be introduced by Royal decree.[108] Following the Explanatory Report the legislature

has linked the derogation in Article 10 to Article 13 of the Directive.[109] The Belgian Act does, however, go beyond the scope of the text of the Directive. The latter provides — in conformity with the jurisprudence of the European Human Rights Court — that the exception is not automatic, and that for every particular case it should be checked to see if the exception constitutes a necessary measure to safeguard the listed interests found in Article 13 of the Directive.[110]

Article 12, §1 introduces grounds to oppose in two situations:

Firstly, the data subject is granted the right to object against the processing of data relating to him for serious and legitimate reasons related to a specific situation, unless the lawfulness of the processing is based on the performance of a contract or is necessary for compliance with a legal obligation. Thus, the data subject has a greater opportunity to oppose the processing of his personal data than is provided in Article 14, 1 of the Directive.

In addition, the opposition right applies in a case where personal data is processed for means of *direct marketing*.[111,112] The data subject can object without charge and free of any motivation opposing the processing of his personal data for this purpose. As has been commented before, this rule can only be effective so far as the data subject has been informed beforehand about the planned processing.

Further, in cases of legitimate opposition the processing commenced by the controller may have to stop including those data. Finally, the new Act restates the rule that everyone is entitled freely to obtain erasure or prohibition of processing of all personal data concerning his person that are incomplete or irrelevant, or of which the registration, the communication or the conservation are forbidden, or are maintained after the permitted period is complete.[113]

The third paragraph of Article 12 states that the controller should — within a month from the lodging of the request — inform the data subject about the completed verifications or removals as well as the *persons*[114] to whom the incorrect, incomplete or irrelevant data are communicated, *as far as he still knows the identity of the addressees and the information about the latter does not seem impossible to obtain or does not create disproportionate difficulty*.

It could be argued that the controller should take the necessary measures to keep details of to whom he distributes the personal data for means of direct marketing. This obligation could be vested on the duty to act carefully and the proper balance between the interests and liberties of the parties.

Automated individual decisions

Article 12 *bis* of the new Act introduces a rule that a decision which produces legal effects for a person, or that significantly affects him, should not *merely* be taken on the ground of an automated processing that is intended to evaluate certain aspects of his personality. The Explanatory Report specifies that "*this disposition should avoid decisions being taken that are directly based on the results of an automated processing, without any human intervention.*"[115] It is further made clear that from the very moment that there is a human intervention between the obtaining of the result(s) of the processing and the taking of the decision the present rule must be respected.[116] Of course, this will only be true as far as the human intervention forms a substantial part of the rationale of the decision reached.

The new Act contains two exceptions to this prohibition. First there is the case where the decision is taken in the frame of a contract. The second exception allows the automated decision if such a decision-making process is granted by Act or any other secondary legal norm. The contract and the legal dispositions should contain appropriate measures to safeguard the legitimate interests of the data subject. At least, the latter should be enabled to table his point of view by effective means[117].

The way in which this article is phrased leaves many "back doors" open. What are "appropriate measures"? What are "legitimate interests" of the data subject? The Belgian legislature was neglectful in not creating more clarity in these important matters. Moreover, the data subject will face difficulties where appeal to and intervention by the Privacy Authorities have a retrospective character. It is both regrettable and alarming that in a modern "Rechtsstaat" the liberties of the citizens are endangered and particularly in this concealed way.

2.5 The responsibilities of the organizations that process personal data

In this section we shall try to give a succinct overview of the internal and external systems of controls that are envisaged by the new data protection Act. In a first sub-paragraph a comment will be given upon the confidentiality and security rules and the duties of that personal data protection officials (internal aspects). In the next section we shall deal with the obligation to notify the supervisory authority (external aspects).

Of course, the controller should also honour many other obligations. These have already been commented upon because they are mirrored in the rights of the data subject and the general rules of lawfulness of the processing. No further elaboration will be offered here.

Confidentiality and security of processing

Article16 contains the measures that should be taken in order to guarantee a confidential and secure processing. The same article of the previous Act already contained an extensive list with obligations so that only some minor adaptations were needed in order to attain conformity with the Directive.

The first paragraph fixes the conditions to be respected when the controller — or his representative in Belgium — delegates the processing to a processor: a processor should be chosen who offers sufficient guarantees as to the technical and organizational measures. The controller should also ensure compliance with those measures by laying down the necessary requirements in a contract with the processor. The same contract should regulate the responsibility between processor and controller, and establish that the processor is acting on behalf of the controller and is held by the same obligations as the latter. Finally, the elements of the contract concerning the protection of the data and the exigencies concerning the measures mentioned in § 3 (cf. *infra* hereafter) should be fixed in written or upon an electronic carrier.

Following the third paragraph, any person having access to personal data and acting under the responsibility of the

controller or processor — as well as the processor himself — may only process these data on the instructions of the controller, unless otherwise legally obliged to do so by Act or secondary legal norm.

The second paragraph lists some specific obligations to be honoured by the controller or his representative. He is responsible for the quality of the processed data and for the organization of limited access to only those persons acting under his authority. He should further inform the personnel about the existence of the data protection Act and its constraints and check to see whether the programs of automated processing are in conformity with the notification given to the Privacy Authority.

The obligation to make what was called under the previous Act "a statement" is omitted in the new Act. A statement is a document describing the character of the processed data, the purpose of the processing, the mutual connections and all other aspects regarding the modalities by which the processing is integrated in the system of informatics and administration of the enterprize. The ratio was firstly to assure the transparency of internal transfers of personal data, and secondly to guarantee to the Privacy Commission that a complete view on the conditions by which the data is processed has been provided. The reason why the legislature left out this obligation is that it was never respected in reality.[118]

The obligation to take appropriate security measures is almost literally taken over from the old data protection Act, though the responsibility for this no longer rests solely on the shoulders of the controller. Furthermore, the processor should take adequate technical and organizational measures necessary to guarantee full security of the data.[119]

Obligation to appoint a Personal data protection official

Article 17 *bis* of the new Act introduces the possibility to appoint a data protection official that can, following the wording of the Directive, exercise internal control of the data protection legislation and otherwise form a point of contact with the Privacy Commission and the outside world.

Unfortunately, the new Act provides for the appointment of this official only as far as the processing contains *specific risks* to the personal rights and freedoms of data subjects. Again, and typical for Belgium, it will be by Royal decree identifying the categories of processing where such an official will be introduced, and the operation required. The instalment of a privacy official implies no exemption from the duty to notify the Privacy Authority.[120]

It could be asked why a processing must first be risky before a privacy official may be appointed? Article 17 *bis* may create confusion between 'official' and 'unofficial' privacy officials.

Obligation to notify the supervisory Authority

The obligation to notify the supervisory Authority already existed in the Act of 8 December 1992. This old disposition was in fact simply retaken and slightly adapted to the exigencies and the new wording of the Directive.

The general rule is that the controller should notify the Privacy Authority before he undertakes one or more complete or partial automated processing of data for a particular or related purpose.[121]

Notification is not needed for processing that relates to the maintenance of a public register that is by the Act or secondary legal norm intended to inform the public and available to be consulted by any member of the public with a legitimate interest. Notification will not, for example, be required for a general list kept up by the record-office of the courts[122].

The following information should be notified: if the processing is established by law, the legal basis; the identification of the controller; the naming of the processing; the purpose or connected purposes of the processing; the categories of sensitive data processed, if any; the categories of recipients; the guarantees provided if personal data is transferred to third parties; the modalities of information about the data subject, of the exercise of the right of access and the measures taken to facilitate this right; the period after which the data may no longer be retained, used or diffused; a general description to evaluate if compliance with security rules is guaranteed; and the reason why the controller relies on a partly or total exemption of the data protection Act.[123] If the processing is ended or if any change is made to the methods of processing, this should also be notified.[124]

The Privacy Commission is in charge of the nature and structure of the notification.[125]

Additional information should be given to the Privacy Authority in case it is planned to send the processed data, even occasionally, abroad.[126] In this case the categories of the data that will be transferred and the destination country should be notified.[127]

Paragraph 8 states that the King can fix the categories of processing to be granted exemption from the obligation to notify in these situations where — taking into account the nature of the processed data — there clearly exists no danger of any encroachment upon the rights and liberties of data subjects provided the categories of processed data, the categories of data subjects, the categories of recipients and the period of conservation are specified.[128] If one falls under the categories of exempted processing, the same information, as mentioned above, should be given to every person requesting.[129]

The ninth paragraph fixes the financial obligation of the controller according to the notification.

The data protection official is thus in contradiction with the Directive not being an alternative to notification but rather an additional measure designed to pursue secure and safe processing.

Finally, the grant by the Privacy Authority and the use of a registration number for every processing is expressly omitted.[130]

With regard to the Privacy Authority, almost nothing has been modified to comply with the provisions relating to the 'Data Protection Authority': the Belgian Privacy Commission will keep its previous competence and composition, except for minor modifications.

With regard to its composition, we should underline the fact that the Chairman of the so-called 'Supervisory Authority for the Crossroad Bank of Social Security' is no longer a member *ex officio* of the Privacy Commission. This decision has been taken in order to modify the relationship between the Privacy Commission and the various sectorial privacy commissions.[131]

As from now, the Privacy Commission will nominate a representative in each sectorial commission who will be entitled to block the decisions (right of *veto*) proposed by these sectorial Commissions.

So, the Belgian Legislature has maintained the broad composition of the Commission following the French model. There is no modification regarding the status of the Commission's employees and their financial autonomy, notwithstanding the express request of the Privacy Commission for a clear functional separation between the controlled processors and their controlling authority.

Finally, the Data Protection Authority has competence to exercise only consultative power, except for two minor exceptions[132] — notwithstanding the increase in power envisaged by the Directive,[133] including those of injunction and decisions.

2.6 Juridical Sanctions and Remedies

The number of Privacy cases before the Courts is quite limited.[134] In one case before the High Court of Justice the problem was to determine whether a simple file constituted a processing of a manual filing system in accordance with the terminology of the previous data protection Act.[135] Certain cases developed before the administrative courts do not refer to the Privacy Act even if data protection questions arose in those cases.

More interesting is the frequent recourse to the specific procedure installed by Article 14 of the data protection Act, before the President of the 1st Instance's Court, acting as 'en référé'. Many complaints against the use of inaccurate data, specifically in the context of consumer credit have been addressed.[136] This specific procedure is characterized by its speed, which has been maintained under the new Act.

Further, Belgian case law is characterized by the frequent use of the action 'en cessation' before the President of the Commercial Court as regards 'unfair competition' which is deduced from illegal processing of nominative data by competitors. So, insurance companies have sued a bank that was processing personal data derived from bank transfers in order to identify advertising markets for insurance services offered by the bank[137]. Independent Car retailers have similarly sued the Car retailers' Federation, which had obtained from the Administration information about car owners for marketing purposes.[138]

With regard to remedies, the new Belgian Act reproduces a long list of criminal sanctions in its Article 15 *bis.* Article 23 of the Directive deals with the liability of the controller.

It is indeed quite important to establish that the Explanatory Report expressly believes that a system of liability without fault (Fr.: 'responsabilité objective') is recognized by this article[139]. The only proof to be furnished by the data subject is evidence that the damage has resulted from a breach of the legal provisions. If the data controller wants to be exempted, he will have to prove either *force majeure*, or fault on the side of the data subject or of a third party.

The efficacy of the new Act can further be increased by the introduction of codes of conduct. Article 44 of the previous data protection Act delegated to the King competence to issue-specific rules about the privacy principles *vis-à-vis* certain sectors. Notwithstanding the failure to use this provision up to now, this possibility is maintained.

Two new sections have been introduced, referring to Article 27 of the Directive. So, trade associations or other bodies representing categories of controllers can submit their professional privacy rules to the opinion of the Privacy Commission.

Undoubtedly, it is regrettable that no code of conduct has ever been submitted to the Data Protection Authority. However, even if the latter developed a weak position in face of the private sector in the past, it could be argued that the new competence recognized by the Act will encourage a new policy of open discussion with trade and other associations.

2.7 Transborder Data Flows

Instead of the previous vague provisions under which Royal decrees can regulate any data flow, including but not exclusively transborder data flows, Articles 25 and 26 of the European Directive are reproduced by Articles 21 and 22 of the new Belgian Privacy Act. Article 21 provides that a transborder data flow is authorized only if the third country in question ensures an adequate level of protection. According to the Privacy Commission's advice, the appreciation of the 'adequacy' of the protection afforded by the third country will be under the sole responsibility of the exporter of the personal data. Undoubtedly, one might imagine that the recommendations adopted by the so-called 'Article 29 Working Group'[140] will have to be respected.

Further, in accordance with Article 25 of the Data Protection Directive, the King has competence, after consultation of the Privacy Commission, to determine a black list of countries to which transfers may be prohibited. Nothing is said about the white list, also provided for in the Directive.

With regard to the two categories of derogations enacted by the Directive: more specifically, the particular cases mentioned in Article 26 (1) and further, the compensation for lack of protection by 'adequate safeguards', notably through contractual means, proposed by Article 26 (2). These are now restated by the new Article 22 of the Belgian Act of 11 December 1998. While there is nothing particular to say about the list of derogations (unambiguous consent, necessary transfers, public interest or legal claims, vital interests, etc.), with regard to the second type of derogations, it is clear that 'adequate safeguards' must be fixed by a Royal decree. The draft version of Royal decree fixes a minimum set of contractual clauses that are supposed to offer the "appropriate safeguards, providing for the liability of the data exporter in the case of violation of privacy". In our opinion, this minimal list would have to be fixed only after a preliminary discussion with the other EU Member States in order to avoid distortions between the national regulations on that point.

3. DATA PROTECTION MEASURES AS IMPLEMENTATION OF DIRECTIVE 97/66/EC AND CONCLUSION

The Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunication sector is currently integrated within the Belgian legal order. The introduction of some articles of Directive 97/66/EC has, however, already been anticipated in Royal decrees and in legislation. These texts form a disparate collection of rules

that have — due to the continuous change and complexity of the telecommunications sector — a quite confused character. A draft of a Bill completing the implementation of the Directive is being conceived, though some principles have not taken a definite form yet, so that a comment here would be too hasty.

The following Articles of the Directive are still waiting for implementation: Article 3; Article 5(2) (registration of communications for business purposes); Article 6 (traffic and billing data)[141]; Article 7 (itemized billing); Article 8 (presentation and restriction of calling and connected line identification)[142]; and Article 12(1) (automated marketing).

Chapter x*bis* of the Act of 21 March 1991 relating to the reform of economic public enterprizes[143] concerning "the secrecy of communications and privacy protection". Article 109 *ter*C[144] states that every person offering vocal or mobile telephone services to end users[145] should, in accordance with technical and financial conditions laid down by the King, delete the data of persons that have indicated a wish not to be mentioned in a directory when the data is transferred for publication. It should be noted that only the advice of the Belgian Institute for Post and Telecommunications services is required to fix the technical and financial conditions though no intervention of the Privacy Authority is provided for, even if these conditions will be a determining factor for the privacy of end users. Persons that are included in lists of end user data that are not intended for the edition of directories but for other purposes (mostly direct marketing) have the right to have their end user data omitted without charge. No legal definition is given for 'end user data', which could render it uncertain if Article 11(1) of Directive 97/66/EC is not effectively implemented.

Article 109 *ter*D of the same Act contains a description of the secrecy of communications. It is remarkable that the secrecy of communication is also protected by the Articles 259 *bis* and 314 *bis* of the Belgian Penal Code.[146] The wording of Article 109 *ter* D is, however, broader because — *inter alia* — the confidentiality of the communication is protected beyond the moment of transmission. In addition to the fact that one needs experience with Sanskrit to comprehend the text of these Acts, it seems from a legislative point of view to be an unnecessary obstruction to regulate one matter by two different legislative instruments.

Article 109 *ter*E formulates some exceptions to the principle of secrecy of communication. The above-mentioned principle does not apply when: (i) the law permits or imposes the accomplishment of the above-mentioned actions; (ii) these acts are necessary to guarantee the good functioning of the network and to assure the good execution of a telecommunications service; and (iii) the acts are carried out to enable the auxiliary services to intervene in cases where their help is needed after the receipt of a request for intervention.

Finally, the use of cryptography is free.[147] Prior to the supply of cryptographic services to the public notification to the Belgian Institute for Post and Telecommunications services was mandatory.

It can be firmly concluded that although the new data protection Act has enlarged the protection principles to a certain extent, the quality of the legislation can be questioned. The new generation of data protection Acts will have to prove their effectiveness and efficacy in a context where new technologies (the Internet, health telematics, biometrics, etc.) are becoming more important and sometimes inextricably entwined. It is regrettable that, on the basis of the experiences of the previous data protection Act, no profound and systematic interdisciplinary research has been done to enhance the quality of the Act. Furthermore, as has been commented many times, the democratic quality of the Act can be questioned given that many fundamental aspects have been left to the goodwill of the King. Deeper research is necessary to sort out what the concrete influences are of the new technologies and the increasing complexity of our conceptualization of modern democracy.

Jan Dhont, CRID, Facultés Universitaires Notre-Dame de la Paix, Namur and
Yves Poullet, Directeur CRID, Facultés Universitaires Notre-Dame de la Paix, Namur

FOOTNOTES

*This article is a slightly revised version of a former publication in the Journal of International Computer Law.

[1]Furthermore, the inviolability of the residence and the confidentiality of the mail are recognized in Articles 15 and 29 of the Belgian Constitution.

[2]Dumortier, J. and Robben, F., *Persoonsgegevens en privacybescherming*, Die Keure-ICRI, Brugge, 1995, p. 8.

[3]See Article 458 of the Belgian Penal Code.

[4]Act of 11 April 1994 concerning the publicity of the administration, *Official Journal*, 30 June 1994.

[5]See Article 662 of the Belgian Civil Code.

[6]Act of 21 March 1991 concerning the reform of some economic enterprizes of the state, *Official Journal*, 27 March 1991.

[7]*Official Journal*, 30 December 1993.

[8]Bill concerning the protection of some aspects of the personal sphere of life, Parl. Doc., Senate, 1975-1976, 846 pp.

[9]*Official Journal*, 21 April 1984.

[10]See the Act of 12 June 1991 concerning the credit of consumers, *Official Journal*, 9 July 1991 and the Act of 19 July 1991 concerning the Public Registers and the Identity Cards, *Official Journal*, 3 September 1991.

[11]The following abbreviations will hereafter be used:
[Explanatory Report]: Explanatory Report, *Doc. Parl.*, Ch. repr., sess. ord. 1997-1998, nr. 1566/1.
[Advice of the Council of State]: Advice of the Council of State, 2 February 1998, *Doc. Parl.*, Ch. repr., sess. ord. 1997-1998, nr. 1566/1.
[Advice of the Privacy Commission/Authority]: Advice nr. 30/96 of 13 November 1996 of the Privacy Commission, *Doc. Parl.*, Ch. repr., sess. ord. 1998-1999, nr. 1566/10.

[12]For a general comment on the Directive 95/46/EC, see Louveaux, S., Poullet, Y. and Willems, V., *A Business Guide to changes in European Data Protection Legislation*, Cullen International (ed.), Kluwer Law International, 1999, 315 pp.

[13]See for instance Royal decree nr. 7 of 7 February 1995, determining the purposes, criteria and the conditions for permitted processing of data as meant by Article 6 of the data protection law of 8 December 1992, *Official Journal*, 28 February 1995.

[14][Explanatory Report], p. 8.

[15]The majority of the discussions concerned the Bill according to the protection of personal data in the context of the activities of the Centre for children that have disappeared (see *infra* nr. 15).

[16]This is almost inevitable at the level of definition, but less defensible for the detailed texts of the specific rules. The Council of State criticized the authors of the Bill *inter alia* for having copied rather than transposed the many rules from the Directive (see [Explanatory Report], p. 91 e.ff.)

[17]The new Act uses the notion *information* in stead of *data*. 'Data' has a more atomistic character in comparison with 'information', which is a more generic notion. Probably this distinction is of a more academic nature.

[18]See Article 1, §5 former version data protection Act.

[19]See Article 1, §1 of the new Act.

[20]Advice nr. 04/97 of 19 February 1997 of the Privacy Commission.

[21]The text of Recital 26 is the following: "*Whereas the principles of protection must apply to any information concerning an identified or identifiable person: whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person: whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable[...].*"

[22][Explanatory Report], p. 12: "*Une information relative à une personne est donc considérée comme donnée à caractère personnel tant que quelqu'un est encore en mesure, par quelque moyen qui puisse raisonnablement être mis en oeuvre, de déterminer à quel individu se rapporte cette information. Sont donc également considérées comme 'données à caractère personnel' les informations codées pour lesquelles le responsable du traitement lui-même ne peut vérifier à quelle personne elles se rapportent, parce qu'il ne possède pas les clefs nécessaires à son identification, lorsque l'identification peut encore être effectuée par une autre personne. Lorsque les informations relatives à des personnes physiques sont rendues anonymes, elles ne perdent donc leur caractère de données à caractère personnel que si le caractère anonyme est absolu et que plus aucun moyen raisonnablement susceptible d'être mis en oeuvre ne permet de revenir en arrière pour briser l'anonymat...*".

The Belgian Privacy Commission seems also to be following on the same track putting it as follows: "*il n'est question, dans ce cas, d'un traitement de données à caractère personnel dans le chef du responsable du traitement que dans la mesure où il dispose de la possibilité pouvant être raisonnablement mise en oeuvre de pouvoir procéder à un décodage via le tiers*" [Advice, p. 4].

[23]This leads thus to the distinction between three categories of data: identifiable data, coded data and anonymous data. The first two categories form a subdivision of 'personal data', while the latter falls outside the scope of the data protection legislation. The draft of Royal decree executing the new Act makes this division in the context of the processing of personal data for statistic, historic and scientific goals.

[24]Compare Article 1,§3 and 1,§4 of the previous data protection Act.

[25]See Article 1, §2 of the new data protection Act.

[26]This implies a necessary rectification of the terminology of the Act of 8 December 1992 where the collection of personal data was not considered to be a part of an *automatic processing* or *the holding of a manual filing system* and so fell outside the scope of the Act. However, an obligation of information to the data subject was arranged in Article 4 for the *collection* of personal data.

[27]This was not the case for the definition of an *automatic processing* in Article 1, §3 of the Act of 8 December 1992.

[28]Under the Act of 8 December 1992 there was much uncertainty. For an *automatic processing* to be constituted, more than one operation was necessary (Article 1, §3 Act of 8 December 1992), however, because the notion of processing was not used in the definition of the *holding of a manual filing system* one could argue that only one operation as listed in Article 1, §4 of the Act of 8 December 1992 should fall under the application of the Act.

[29]This seems to be confirmed by the [Explanatory Report], 13: "*Une extraction, par exemple, ou une consultation unique d'un fichier contenant des données à caractère personnel constitue également un traitement auquel s'appliquent les dispositions de la loi.*"

[30]See for this Leonard, Th. and Poullet, Y., "La protection des données à caractère personnel en pleine (r)evolution: la loi du 11 décembre 1998 transposant la Directive 95/46/CE du 24 octobre 1995", J.T., 1999, to be published soon; Boulanger, M.-H., and De Terwangne C., "Internet et le respect de la vie privée", in *Internet face au droit*, Diegem-Namur, Story scientia-C.R.I.D., Cahiers du C.R.I.D., n°12, 1997, 198-199.

[31]Dumortier, J. en Robben, F., *Persoonsgegevens en privacybescherming — commentaar op de wet tot bescherming van de persoonlijke levenssfeer*, 1995, Die Keure-ICRI, Brugge, 68.

[32]See Article (13) 9, §1 and §2 (obligation to inform), Article (14) 10, §1 (right of access) and Article (24)17, §3, 5° (obligation of notification) of the Act of 11 December 1998 that all speak about *the purposes of the processing*. In contra-distinction with the French text — and the Directive — utilizes the Dutch version of the Act in Article 1, §4 purpose in singular form when defining the 'controller'.

[33]Firstly, the [Explanatory Report] (p. 55) correctly connects the notions 'purpose' and 'processing': "*(...) Cette formulation concerne la signification attribuée à la notion de 'traitement' dans la loi actuelle, ainsi que le rapport établi entre cette notion et les finalités du traitement. (...) Les notions de 'finalité' et 'traitement' coïncident donc en grand partie.*"

Though further on it is (correctly) mentioned that a sole *operation* can constitute a processing which leads, however, to the wrong conclusion that this is *automatically* the case. By automatically associating an 'operation' with a 'processing', one loses the purpose for which the processing is done, which leads to the conclusion that the Legislator contradicts itself: "*La directive utilise une série de notions plus précises. Un traitement est, comme dans le language usuel, défini comme toute opération effectuée avec des données à caractère personnel. Au sens de la directive, il arrive donc souvent que de très nombreux traitements (read: 'opérations') soient effectués pour la même finalité.*" [Explanatory Report, p. 55].

[34]See Article 1, §3 Act of 11 December 1998: "*tout ensemble de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionelle ou géographique.*"

[35]In the past, a highly critical judgement of a Belgian lower court was cited. It ruled that medical files in a hospital did not fall under the scope of the data protection legislation, even if specific Belgian legislation determines that these files should be held for reasons of administration and control (Court of first instance, Hasselt, 2 October 1997, *Rev. Dr. Santé*, 1997-1998, 333 e.ff.).

[36][Advice], p. 2.

[37]The highest Belgian Court decided already on these matters, but the judgement did not put forward any more clarifying criteria, see Court of Cassation, 16 May 1997, *J.T.*, 1997, p. 779.

[38]See Article 1, §4 of the Act 11 December 1998: "*La personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les*

finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le responsable du traitement est la personne physique, la personne morale, l'association de fait ou l'administration publique désignée comme responsable du traitement par ou en vertu de cette loi, de ce décret ou de cette ordonnance."

[39]Compare with the definition of *controller* in Article 2 d of the Directive.

[40]In the French text purposes.

[41]See Boulanger M.-H., De Terwangne, C. and Leonard, Th., "La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel", *J.T.*, 1993, 373, n° 16; Leonard, Th. and Poullet, Y., "La protection des données à caractère personnel en pleine (r)evolution: la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995", J.T., 1999 (to be published soon).

[42][Explanatory Report], p. 15: "*Selon le texte de la directive un traitement peut également relever de la responsabilité de plus d'une personne. Plusieurs personnes ou associations de fait peuvent être co-responsables d'un même traitement.*"

[43]See Article 1, §5 of the new Act.

[44]See Article 1, §5 *in fine* of the new Act.

[45]See Article 1, §6 of the new Act.

[46]*Official Journal*, 15 March 1996.

[47]See Article 1, §7 of the new Act.

[48]See Article 13 of the new Act.

[49]See [Explanatory Report], p. 16.

[50]See Article 24 of the new Act.

[51]See [Explanatory Report], p. 16.

[52]See Article 1, §8 of the new Act.

[53]See Article 9 and 10 of the new Act.

[54]Exception should be made in a situation where the name of a legal person matches the name of a physical person, in which case the Act will be applicable.

[55]It might be supposed that the most primarily personal data (name, address, date of birth, etc.) does not fall under the scope of the Act of 8 December 1992 because this information is mentioned in the Public Registers that are there fundamentally for publicity (see Article 45 e.ff. Belgian Civil Code).

[56]See Advice nr. 09/95, 5 April 1995 of the Belgian Privacy Protection, *Rapport d'Activité 1994-1995*, pp. 19-20; Recommandation du Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, "Legislation sur la protection des données et médias", nr. 1/97 du 25 février 1997, Commission Européenne, DG XV, 5012/97-FR (http://europa.eu.int/comm/dg15/fr/media/dataprot/wpdocs/index.htm).

[57]It is submitted that there is a different level between the two categories; journalism is supposed to give (more than literature) a description of reality in which case more severe rules for processing for journalistic means could be upheld. See [Explanatory Report], p. 19.

[58]In the Explanatory Report it refused to explain clearly what the legal meaning is of these three purposes *because the interpretation of these notions, issued by a European Directive, belongs in last instance to the European Court of Justice*, [Explanatory Report], p. 19.

[59]See Article, 3, §3, a of the new Act.

[60]See Article, 3, §3, b of the new Act

[61][Explanatory Report], pp. 21-22.

[62]It is indeed not unrealistic to suppose that the source where the journalist gets his information will fade away if the duty to inform is applied strictly. Furthermore, is it logical that undercover practices will become eliminated; [Explanatory Report], p. 22.

[63]See Article 3, §3, c) of the new Act.

[64]See Article 3, §3, d) of the new Act.

[65]See Article 3, §4 of the new Act.

[66]It is hard to imagine how one could bring an action against these authorities if the citizen does not know what personal data and for what means it is processed.

[67]For a detailed comment on the protection of privacy in the public security sector, see Poullet, Y. and Havelange, B., "Secrets d'Etat et Vie Privée: ou comment concilier l'inconciliable?", colloquium organized by the Comity R, 20 January 1998, *Secret d'Etat ou transparance*, Bruxelles, to be published, nr. 15.

[68]Hereafter called 'the Centre'. The Centre is an establishment of public utility constituted by an Act of 25 June 1997. The mission of this Centre is to deliver active help to the recovery of disappeared or kidnapped children, to prevent and fight against the disappearance and sexual exploitation of children. On 30 March 1998, a Protocol for collaboration was signed between the representatives of the Centre, the Minister of Justice and the five General State Attorneys (see the text of it in the annexes of the Report of the Commission of Justice, *Doc. Parl.*, Ch. repr., sess. ord. 1998-1999, n° 1566/10, p. 203). During the passage of this Protocol, it became obvious that the Centre could only do its job if the personal data of victims, suspects and offenders were collected and registered. The advice of the Privacy Commission was solicited, but the result was negative (Advice nr. 10/98, 12 March 1998, in annexes of the Report of the Commission for Justice, *Doc. Parl.*, Ch. repr., sess. ord. 1998-1999, nr. 1566/10, p. 167). The advice denounced certain collection methods and many forms of processing of sensitive data that were envisaged. The legal basis seemed to give way to some exceptions to the privacy protection rules. The different exceptions were bundled in a distinct Bill (Projet de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement des données à caractère personnel, *Doc. Parl.*, Ch., s.o. 1997-1998, n° 1586/1). These exceptions were then inserted in the Bill, which led to the data protection Act.

[69]See Art. 9, 10, §1 and 12 of the new Act.

[70]The old data protection law contained the following provision: "The present law is applicable to:
1° the holding of a manual filing system in Belgium;
2° every automated processing, even if the operations are wholly or partly effected abroad, as far as the processing is directly accessible in Belgium by means proper to the processing."

[71]See Article *3bis*, 1° of the new Act.

[72][Explanatory Report], p. 26.

[73]For a more thorough analysis of this criterion, see Leonard, Th. and Poullet, Y., "la protection des données à caractère personnel en pleine (r)evolution: la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995", l.c., p. 12.

[74]This Article should be read with Recital 20 of the Directive in mind: "*Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice.*"

[75]Under "means" the following Explanatory Report should be understood: "every possible equipment, such as computers, telecommunication machinery, print units, etc., with explicit exclusion of means

that are uniquely used for the transit of personal data over the territory, such as cables, routers, etc.", [Explanatory Report], p. 27.

[76]See Boulanger, M.-H. and De Terwangne, C., "Internet et le respect de la vie privée", *op. cit.*, pp. 200-204.

[77][Explanatory Report], p. 27.

[78]Recital 10 of the draft version of the Directive envisaged explicitly a transfer in order to escape the obligations of it. See Com (92) 122 final — Syn 287, *J.O.C.E.*, 27 November 1992, nr. C 311, p. 33.

[79]The Belgian Act does not permit any exception to this principle. This position will create problems as regards certain processings like those operated by the State Security's Services. See on that point Havelange, B. and Poullet, Y., "Secrets d'Etat et Vie Privée: ou comment concilier l'inconciliable?", colloquium organized by the Comity R, 20 January 1998, *Secret d'Etat ou transparance*, Bruxelles, to be published.

[80]This principle implies that the processing of personal data may only pursue purposes that are compatible with the initial purpose of the Data collection. The "compliance principle" means that only purposes be pursued which are compatible with the initial purpose of the data collection. The evaluation of the compatible use will be done, under Art. 4, §1, 2° of the new Act, either by the legitimate expectations of the data subject, or by the regulations. As regards the second hypotheses, it implies that a modification of purpose will be considered as legitimate, each time it is imposed by a regulatory measure. Following the terms of the Explanatory Report, the use for secondary means that is incompatible with the initial purpose of the processing requires the explicit consent of the data subject.

[81]See Article 6 of the previous Act.

[82]See Article 7 of the previous Act.

[83]See Article 8 of the previous Act.

[84]The Minister of Justice has proposed, however, that the criterion would have to be applied with reasonable care, which means that the application of Article 6 will be elicited only when the sensitive nature of the data can be deduced with certainty of quasi certainty. For example, if a person is purchasing a Bible, this operation does not reveal definitively his religious belief. This interpretation has been broadly criticized by Leonard, Th. and Poullet, Y., *Op. cit.*, nr. 35 and ff.

[85]So, administrative data processed for the reimbursement of medical treatment or prescriptions should not necessarily be regarded as sensitive data.

[86]These provisions should be read with the Recommendation R (97)5 of the Comity of Ministers of the Council of Europe regarding the protection of medical data.

[87]A Royal decree will determine the list of persons to be considered as "healthcare professionals".

[88]See Article 39, 3 of the new Act.

[89]"To collect" has a rather active connotation while "to obtain" also makes allusion to the situation where the data subject spontaneously releases his personal data. See [Explanatory Report], p. 44.

[90]These two hypotheses were regulated before by Articles 4 and 9 of the previous data protection Act.

[91]Article 9, §1 (a)-(c) and §2 (a)-(c) of the new Act.

[92]Article 9, §1 (d) and §2 (d) of the new Act.

[93]Article 9, §1 (e) and §2 (e) of the new Act.

[94]The obligation to inform correctly is considered to be an "obligation de résultat". The means by which the information will be communicated as well as the content of the information — to a certain level — have to be appreciated by the controller, [Explanatory Report], p. 45. The question, however, will be whether the controller can always correctly estimate what information should be given to guarantee a loyal processing. The criterion to be followed is that of complete openness and transparency. The Privacy Commission put it as follows: "*Ainsi on pourrait dire que, si la collecte de données se déroule en grande partie au profit des tiers, un traitement loyal suppose que l'identité des destinataires soit révélée. On pourrait encore préciser, lors de la collecte de données à des fins commerciales qu'un traitement loyal suppose que l'identité de la personne concernée soit informée du fait qu'il peut s'opposer à ce traitement. Enfin on pourrait affirmer que, lors de la collecte de données pouvant avoir de lourdes conséquences pour la personne concernée (par exemple, concernant le droit à une indemnité ou une appréciation de la solvabilité), il est essentiel que l'attention de la personne concernée soit attirée sur son droit d'accès et de rectification.*"

[95][Explanatory Report], p. 46.

[96][Advice], §28.

[97]There is no indication in the new Act about what should be understood under the notion "population research". Article 7 mentions that health data can be processed for this purpose, though it is semantized as a category apart from "scientific research". A strict legalistic reading of the new Act leads to the contradictive assessment that the exception to the finality principle as provided for scientific research is not valid for "population research", in which case this kind of research is made totally impossible. Moreover, as far as no further specific obligations are mentioned in the new Act for "population research", there exists a risk that researchers will try in some cases to qualify their research activities as "population research", e.g. systematic research done by a group of hospitals on their population.

[98]See Article 9, §2 (a) of the new Act.

[99]A draft of the Royal decree is in the making and establishes a specific regime for the processing of personal data for scientific, historical and statistical means. A distinction will be made between anonymous data, encoded data and identifiable data. Information will in principle always be needed when working with encoded or identifiable data.

[100]See Article 9, §2 (b) of the new Act. With secondary legal norms we allude to all forms of legislation that are not discussed in a democratic forum, e.g. Royal decrees, Ministerial orders, etc.

[101]See Article 10, §1 of the new Act.

[102]This section was introduced after a proposal of the Privacy Commission ([Advice], p. 17, nr. 31) and permits the controller to rely on a health professional to give perusal to the data subject (mostly patients). The Commission preferred this formulation instead of the wording that the controller could refuse access to the data if this would heavily damage the health of the latter (therapeutic exception), because it was considered that the controller would rely (illegitimately) to fix on this exception and so hollow this right. It is, however, not very clear that the new formulation proposed by the Commission will succeed in establishing more medical transparency, as far as the controller can demand indirect access in all cases. It would have been better that a refusal of direct access would be motivated, be it purely internal, by the fact that access would harm the health of the data subject. One could also ask if it would not have been more correct to give access by bypassing a *physician* and not by any arbitrarily chosen health professional.

[103]See [Explanatory Report], p. 49.

[104]This formulation leads to the conclusion that if measures or conclusions could be taken vis-à-vis groups of data subjects, this will not prevent the data subjects claiming a right of access.

[105]For a thorough analysis of the processing of health data for scientific and statistical purposes, see Dhont, J. and Poullet, Y. *De*

verwerking van medische persoonsgegevens voor statistische en medische doeleinden, 1998, SSTC, Brussel, 105 p.

[106]Cf. *supra* nrs. 13-15.

[107]See Article 13.

[108]The [Explanatory Report] (p. 53) gives the following ratio: "*La solution proposée est de prévoir une communication plus flexible pour les traitements de données gérés par les services de police en vue de procéder à des contrôles d'identité. C'est précisément dans ces cas que la personne concernée est parfois confrontée à des erreurs à son propos, de sorte qu'il doit pouvoir être informée que les données ont été corrigées, sans pour autant communiquer les données mêmes (...)*".

[109]See [Explanatory Report], p. 52.

[110]See Havelange, B. and Poullet, Y., *op. cit.*

[111]The question will be what kind of activities should be qualified as *direct marketing*. The legislature seems, in every case, to have followed a quite broad understanding of this notion, which exceeds the *expectations* of customers; see [Explanatory Report], p. 47.

[112]There existed before a practice to recognize *de facto* (though limited) a right of opposition. Data subjects could inscribe what is called the 'Robinson list' containing the identity of all persons that opposed the use of their personal data for direct marketing purposes. This initiative organized by the Belgian Direct Marketing Association was only of limited success because not all enterprizes are connected to the association. Further, this practice was not legally enforceable.

[113]See Article 12, §1, fourth section of the new Act.

[114]The new Act does not use here the notion 'third party' or 'recipient'. No specific explanation is given for the used vocabulary. Because the word 'person' has a more general connotation than 'third party' and 'recipient' it could be envisaged that it covers a broader meaning.

[115]See [Explanatory Report,] p. 17.

[116]See [Explanatory Report,] p. 17; it may be questioned whether or not the data subject should be informed about the process in which the decision or evaluation of his personality is completed.

[117]See Srticle 12 *bis*, second section of the new Act.

[118][Explanatory Report], p. 54.

[119]See Article 16, §4 of the new Act. It is further mentioned that adapted norms according to the security of informatics can be issued by Royal decree for all or certain categories of processing. This makes it possible to provide supplementary protection in a continuously evolving technological context.

[120][Explanatory Report], p. 56.

[121]See cf. *supra*, nr. 6.

[122]See Article 719 of the Belgian Judicial Code.

[123]See Article 17, §3 of the new Act.

[124]See Article 17, §7 of the new Act.

[125]See Article 17, §5, second sentence of the new Act.

[126]See Article 17, §6 of the new Act.

[127]It is not clear what is meant by "send" or "transferred". It is more realistic to read these words as meaning the 'physical transferral of information'. Otherwise, this paragraph could never be honoured. Think, for instance, of personal data placed on a server situated on the Belgian territory.

[128]A regime of exemptions existed already under the previous Act and was more precisely established in the Royal decree nr. 13 of 12 March 1996, *Official Journal*, 15 March 1996.

[129]See Article 17, §8 of the new Act.

[130][Explanatory Report] p. 57.

[131]Up to now, only one sectorial commission has been created for the Social Security Sector but others (e.g. for the Credit Sector or for the National Registre) have been envisaged.

[132]Firstly, with regard to the 'homologation' or approvals of the Codes of conduct presented by the Trade associations; secondly, Article 19 does grant a power of injunction to the Privacy Commission in case of incomplete or false notice of a controller.

[133]On that point, see Poullet, Y., "L'autorité de Contrôle: 'Vues' de Bruxelles", R.I.S.A., 1999, to be published.

[134]See the Case law review published by Buyle, J.-P., Lannoye, L., Poullet, Y. and Willems, V., L'informatique (1987-1944), *J.T.*, 1997, p. 205 and ff.

[135]Cf. *supra*, nr. 7, Cass., 16 May 1997, *J.T.*, 1997, p. 779.

[136]About this and about the specificity of this procedure, see Leonard ,Th., "La loi du 8 décembre 1992 relative à la protection de la vie privée: limite du champ d'application et procédure contentieux", Civ. Brux., prés., 22 March 1994, *J.T.*, 1994, p. 883.

[137]Commercial Court Antwerp, 7 July 1994 and Commercial Court Brussels, 15 September 1994, *Computerrecht*, 1994, note Dumortier, J. and Robben, F., p. 244.

[138]Comm. Brux., 20 March 1995, commented by Poullet, Y. in Buyle, J.-P., Lannoye, L., Poullet, Y. and Willems, V., *L'informatique* (1987-1944), *J.T.*, 1997, p. 205 and ff.

[139][Explanatory Report], p. 53.

[140]See the Working Document adopted by the Working Group, 14 July: Transborder Data Flows: implementation of Article 25 and 26 of the Data Protection Directive. See also, Havelange, B. and Poullet, Y., *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data*, Luxembourg, Office for Official Publications of the European Communities, 1998, ISBN 92-828-4304-1.

[141]It could be purported that Article 109terD, 3° and 4° of the Act of 21 March 1991 concerning the reform of some economic public enterprizes answers (however, only) partially to the requisites of Article 6(1) of the Directive 97/66/EC. The text of this Article is the following: "*Sous réserve de l'autorisation de toutes les autres personnes directement ou indirectement concernées par l'information, l'identification ou les données visées ci-après, il est interdit à quiconque, qu'il agisse personnellement ou par l'entreprise d'un tiers: 3° de prendre connaissance intentionnellement de données en matière de télécommunication, relatives à une autre personne; 4° de révéler ou de faire usage quelconque de l'information, de l'identification et des données obtenues intentionnellement ou non, et visées aux 1°, 2°, 3° de les modifier ou de les annuler.*"

[142]Exception should be made for Article 8(1) of the Directive that is transposed by Article 9, §3 of the Royal decree of 22 June 1998 concerning the settlement of specifications applied to the vocal telephone services and the procedure regarding the allowance of individual licences, *Official Journal*, 15 July 1998. Furthermore, Article 105 sexies of the Act of 21 March 1991 transposes Article 8,(6) of the Directive.

[143]*Official Journal*, 27 March 1991.

[144]Changed recently by Article 9 of the Royal decree of 4 March 1999, *Official Journal*, 14 April 1999. Although the King is by Act of 1997 authorized to fix these measures, it could be asked if a regulation by Act of Parliament was not necessary as far as these measures imply a curtailment of a fundamental liberty of the citizen.

[145]An end user is defined as follows: "personnes qui utilisent ou demandent un service de télécommunications pour leurs besoins propres." (Article 68, 21° Act of 21 March 1991).

[146]This Article is introduced by Article 2 of the Act of 30 June 30 1994, *Official Journal*, 24 January 1995.

[147]See Article 109 *terF* of the Act of 30 June 1994.